# Security , hacking, threats & tools for security

N.Anupama
Asst Professor
ANUCET
ANU

# Content

- Introduction to security
- Features of security
- Hacking
- Security threats
- Tools to provide security
- Conclusion

# Security

Security is the protection of assets.

The three main aspects are:

- Prevention
- Detection
- re-action

- Information can be stolen – how to prevent it.
- Confidential information may be copied and sold - but the theft might not be detected
- The criminals try to attack and the system should react to stop it.

# Types of Security

- **Computer Security** deals with the prevention and detection of unauthorised actions by users of a computer system.
- **Network security** prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.
- **Web security** deals specifically with security of websites, web applications and web service.
- Features of security
  - Confidentiality
  - Integrity
  - Availability
  - Non-repudiation
  - Authentication
  - Access Controls
  - Accountability

# Features of security

- Confidentiality
  - Confidentiality is keeping information secret or private.
  - The prevention of unauthorized disclosure of information.
  - Confidentiality might be important for military, business or personal reasons.
- Integrity
  - Integrity means that there is consistency in the system - everything is as it is expected to be.
  - Integrity is the authorised writing or modification of information.
  - Data integrity means that the data stored on a computer is the same as the source documents.

# Features of security

- Availability
  - Information should be accessible and useable upon appropriate demand by an authorized user.
  - Availability is the prevention of unauthorized withholding of information.
- Non-repudiation
  - Non repudiation is a method of guaranteeing message transmission between parties via digital signature and/or encryption.
  - Non repudiation is often used for digital contracts, signatures and email messages.
  - A **non-repudiation** service that provides assurance of the origin or delivery of data in order to protect the sender from denial of service by receiver.

# Features of security

- Authentication
  - Authentication is a process in which the credentials provided are compared to those on file in a database of an authentication server.
  - If the credentials match, the process is completed and the user is granted authorization for access.
  - Authentication proves that you are who you say you are, where you say you are, and the time you say it is.

# Features of security

- Access Controls
  - The limitation and control of access through identification and authentication.
  - A system needs to be able to indentify and authenticate users for access to data, applications and hardware.
  - In a large system there may be a complex structure determining which users and applications have access to which objects.

# Features of security

- **Accountability**
  - It guarantees that all operations carried out by individuals, systems or processes can be identified (identification) and that the trace to the author and the operation is kept .
  - Every individual who works with an information system should have specific responsibilities for information assurance.
  - One example is the policy statement that all employees must avoid installing outside software on a company-owned information infrastructure. The person in charge of information security should perform periodic checks to be certain that the policy is being followed.

# Hacking

- Hacking is unauthorized intrusion into a computer or a network.
- The person engaged in hacking activities is generally referred to as a hacker.
- This hacker may alter system or security features to accomplish a goal that differs from the original purpose.

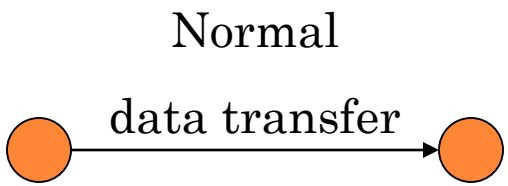
# Types of hacking

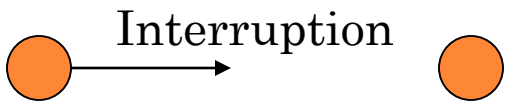
- Local hacking
  - It is done from local area where we have physical access.
  - We can use hard disk and pen drives to install viruses and can hack.
- Remote hacking
  - Remote hacking is done remotely by doing ip spoofing, rootkits etc to get access to the system.
- Social Engineering
  - It is the act of manipulating  people to perform actions or modifying or copying confidential information.

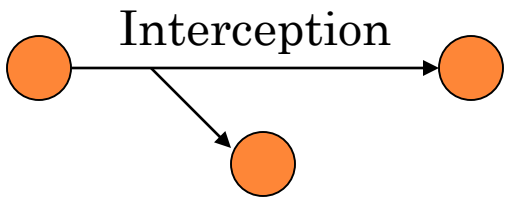
# Types of hacker

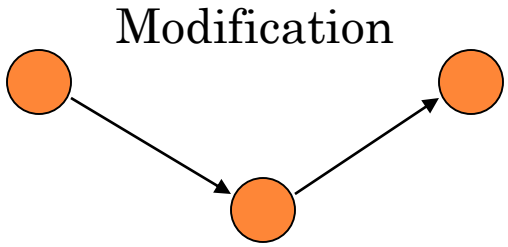
- White hat hacker
  - Ethical hacker a good guy to strengthen the security system.
- Black hat hacker
  - Bad guy or malicious person or the craker who does unauthorized access to the system for wrong intension.
- Grey hat hacker
  - Performs both the operations.
- Hackers use all the modes of threats to hack the system or network or the web.

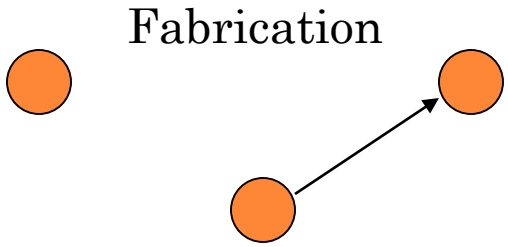
# What hackers do?



# Threats to computer security

- Viruses
- Worms
- Trojan horse

# Computer viruses

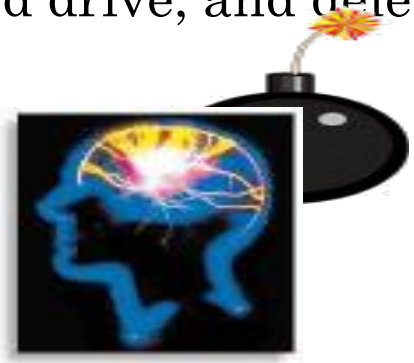
- Computer virus refers to a program which damages computer systems and/or destroys or erases data files
- Types of viruses
  - Time bomb
  - Logic bomb
  - Boot sector virus
  - Macros virus
  - Script virus

# Time Bomb

- A **time bomb** is a malicious program that is programmed to "detonate" at a specific **time** and release a **virus** onto the computer system or network.
- Time bombs are commonly used in pre-release software.
- when the manufacturer of the software does not want the version being used after the final release date then the time bomb detonates.

# Logical Bomb

- A **logical bomb** is a destructive program that performs an activity when a certain action has occurred.
- It is a piece of code inserted into an operating system or software application that implements a malicious function after a certain amount of time, or specific conditions are met.
- They perform actions like corrupting or altering data, reformatting a hard drive, and deleting important files.



- **Boot Sector Virus**
  - A **boot sector virus** infects boot sector of computers. During system boot, boot sector virus is loaded into main memory and destroys data stored in hard disk
- **Macro Virus**
  - A **macro virus** is associated with application software like word and excel. When opening the infected document, macro virus is loaded into main memory and destroys the data stored in hard disk
- script viruses
  - A script viruses are written using the Visual Basic Scripting edition (VBS) and the JavaScript programming languages. These attack the web pages.

# Worm

- A worm has similar characteristics of a virus.
- Worms are also self-replicating.
- Worms are standalone and when it is infected on a computer, it searches for other computers connected through a local area network (LAN) or Internet connection.
- When a worm finds another computer, it replicates itself to the new computer and continues to search for other computers on the network to replicate.
- A worm normally consumes much system resources including network bandwidth, causing network servers to stop responding.

# Worm

- Different types of Computer Worms are:
  - **Email Worms:** Email Worms spread through infected email messages as an attachment or a link of an infected website.
  - **Instant Messaging Worms:** Instant Messaging Worms spread by sending links to the contact list of instant messaging applications.
  - **Internet Worms:** Internet worm will scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. If a computer is found vulnerable it will attempt to connect and gain access to them.
  - **File-sharing Networks Worms:** File-sharing Networks Worms place a copy of them in a shared folder and spread via P2P network.

# Trojan Horse

- **Trojan Horse** is a destructive program. It usually pretends as computer games or application software.
- If executed, computer system will be damaged by Data Modification, Deletion, Blocking, Modifying, Copying, Disruptions ,Computer performance
- Types of Trojans
  - **Backdoor**
  - **Rootkit**
  - **DDoS**
  - **Banker**
  - **FakeAV**
  - **Ransom**
  - **Downloader**
  - **Spy**

# Trojan Horse

- **Backdoor:**

  Gives unauthorized user remote control of a computer. Once installed on a machine, the remote user can do anything they wish with the infected computer. Trojan-infected computers work for criminal activity.

- **Rootkit:**

  Programmed to conceal files and computer activities, rootkits are often created to hide further malware from being discovered. Normally, this is so malicious programs can run for an extended period of time on the infected computer.

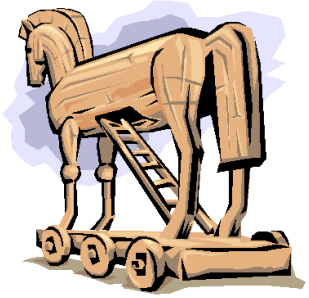
- **DDoS:**

  A sub sect of backdoor Trojans, denial of service (DoS) attacks are made from numerous computers to cause a web address to fail.

- **Banker:**

  Trojan-bankers are created for the sole purpose of gathering users' bank, credit card, debit card and e-payment information.

# Trojan Horse



- **FakeAV:**
  - This type of Trojan is used to convince users that their computers are infected with numerous viruses and other threats in an attempt to extort money. Often, the threats aren't real, and the FakeAV program itself will be what is causing problems in the first place.
- **Ransom:**

  Trojan-Ransoms will modify or block data on a computer either so it doesn't work properly or so certain files can't be accessed. The person disrupting the computer will restore the computer or files only after a user has paid a ransom. Data blocked this way is often impossible to recover without the criminal's approval.
- **Downloader:** These are programmed to download and install new malicious programs onto a computer.
- **Spy:** This type of Trojan horse will be invisible to the user while he or she goes about their daily routines. They can collect keyboard data, monitor program usage and take screenshots of the activity performed on the computer.

# Difference between virus worm and Trojan horse

- Computer Virus:
  - Needs a host file
  - Copies itself
  - Executable
- Network Worm
  - No host (self-contained)
  - Copies itself
  - Executable
- Trojan Horse
  - No host (self-contained)
  - Does not copy itself
  - Imposter Program

## Other threats

Address Book theft

DNS Poisoning

Zombies, IP Spoofing

Password Grabbers

Ploys

Scams

Hijacked Home Pages

Buffer Overruns

Password Crackers

Hoaxes

Pop-Ups

Spam

# Other threats

- Address Book theft
  - Someone who has your e-mail address in their Address Book actually has the malware on their computer and are then sent along to someone else for the purpose of sending spam e-mails.
- Hizaked home page
  - Browser hijacking is a type of online fraud.
  - Scammers use malicious software (malware) to take control of your computer's Internet browser and change how and what it displays when you're surfing the web.
- DNS poisoning/ DNS spoofing
  - It is a form of computer hacking in which corrupt Domain Name System data is introduced into the DNS resolver's cache, causing the name server to return an incorrect IP address.
  - This results in traffic being diverted to the attacker's computer

# Other threats

- Buffer overrun
  - A **buffer overrun** is essentially caused by treating unchecked, external input as trustworthy data.
  - Copying unchecked, input data into a stack-based **buffer** is the most common cause of exploitable faults.
- IP spoofing
  - IP spoofing, also known as IP address forgery or a host file hijack.
  - It is a hijacking technique in which cracker masquerades as a trusted host to conceal his identity, spoof a Web site, hijack browsers, or gain access to a network.

# Other threats

- Zombie
  - zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse program and can be used to perform malicious tasks of one sort or another under remote direction.
- Password Crackers
  - A password cracker is an application program that is used to identify an unknown or forgotten password to a computer or network resources. It can also be used to help a human cracker obtain unauthorized access to resources.

# Other threats

- Password grabbers
  - These are the programs that can be planted on the target computer and can run in background with out computer users knowledge.
  - These programs record the keys pressed and can be used for getting authentication.
- Hoaxes
  - A computer virus hoax is a message warning the recipients of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipients to forward it to everyone they know.
- Ploys
  - Computer games are dangerously addictive and contain powerful psychological devices designed to make some fans play compulsion. Hence these games contain virus causing the threats.

# Other threats

- Pop ups
  - Pop-up ads or pop-ups are often forms of online advertising on the World Wide Web intended to attract web traffic or capture email addresses.
- SPAM
  - Spam is considered to be electronic junk mail or junk newsgroup postings.
  - Some people define spam even more generally as any unsolicited email.
  - Mails sent form unknown emails.

# Actions/tools to provide security

1. Install OS/Software Updates
2. Run Anti-virus Software
3. Prevent Identity Theft
4. Turn on Personal Firewalls
5. Avoid Spyware/Adware
6. Protect Passwords
7. Back up Important Files

# Installing OS updates

- Updates-sometimes called *patches*-fix problems with your operating system (OS) (e.g., Windows XP, Windows Vista, Mac OS X) and software programs (e.g., Microsoft Office applications).

- Most new operating systems are set to download updates by default. After updates are downloaded, you will be asked to install them. Click yes!

- To download patches for your system and software, visit:
  - Windows Update: http://windowsupdate.microsoft.com to get or ensure you have all the latest operating system updates only. Newer Windows systems are set to download these updates by default.
  - Microsoft Update: http://www.update.microsoft.com/microsoftupdate/ to get or ensure you have all the latest OS **and** Microsoft Office software updates. You must sign up for this service.
  - Apple: http://www.apple.com/support
  - Unix: Consult documentation or online help for system update information and instructions.

- Be sure to restart your computer after updates are installed so that the patches can be applied immediately.


# Run Anti-Virus Software

- To avoid computer problems caused by viruses, install and run an anti-virus program.
- Periodically, check to see if your anti-virus is up to date by opening your anti-virus program and checking the *Last updated:* date.
- Anti-virus software removes viruses, quarantines and repairs infected files, and can help prevent future viruses.

# Prevent Identity Theft

- Don't give out financial account numbers, Social Security numbers, driver's license numbers or other personal identity information unless you know exactly who's receiving it.
- Never send personal or confidential information via email or instant messages as these can be easily intercepted.
- Beware of phishing scams - a form of fraud that uses email messages that appear to be from a reputable.
- Order a copy of your credit report from each of the three major credit High Mark Credit Information Services, CIBIL, Experian & Equifax.
- Reports can be ordered online at each of the bureaus' Web sites. Make sure reports are accurate and include only those activities you have authorized.

# Turn on Personal Firewalls


- Check your computer's security settings for a built-in personal firewall. If you have one, turn it on. Microsoft Vista and Mac OSX have built-in firewalls. For more information, see:
  - Mac Firewall
  - (docs.info.apple.com/article.html?path=Mac/10.4/en/mh1042.html)
  - Microsoft Firewall (www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx)
  - Unix users should consult system documentation or online help for personal firewall instructions and/or recommendations.
- Once your firewall is turned on, test your firewall for open ports that could allow in viruses and hackers. Firewall scanners like the one on http://www.auditmypc.com/firewall-test.asp simplify this process.
- Firewalls act as protective barriers between computers and the internet.
- Hackers search the Internet by sending out pings (calls) to random computers and wait for responses. Firewalls prevent your computer from responding to these calls.

# Avoid Spyware/Adware

- Spyware and adware take up memory and can slow down your computer or cause other problems.
- Use Spybot and Ad-Aware to remove spyware/ adware from your computer.
- Watch for allusions to spyware and adware in user agreements before installing free software programs.
- Beware of invitations to download software from unknown internet sources.

# Protect Passwords

- Do not share your passwords, and always make new passwords difficult to guess by avoiding dictionary words, and mixing letters, numbers and punctuation.
- Do not use one of these common passwords or any variation of them:, abc123, letmein, password1, iloveyou1, (yourname1).
- Change your passwords periodically.
- When choosing a password:
  - Mix upper and lower case letters
  - Use a minimum of 8 characters
  - Use mnemonics to help you remember a difficult password

# Back Up Important Files

- Reduce your risk of losing important files to a virus, computer crash, theft or disaster by creating back-up copies.
- Keep your critical files in one place on your computer's hard drive so you can easily create a back up copy.
- Save copies of your important documents and files to a CD, online back up service, flash or USB drive, or a server.
- Store your back-up media in a secure place away from your computer, in case of fire or theft.
- Test your back up media periodically to make sure the files are accessible and readable.

# Conclusion

- War between the good and evil and the battle field is your computer.
- The war is won against evil of proper security measures are taken.


thank
you